36. (New) The method according to claim 21, wherein the decryption stage is carried out using a cryptoprocessor integrated in the portable object.

37. (New) The method according to claim 29, wherein the method comprises an additional stage comprising executing one executable code portion included in the useful data zone, said code portion including application data.

REMARKS

The claims have been amended to remove multiple dependencies. New claims 35-37 have been added. No amendments have been made for reasons relating to patentability. No new matter has been introduced by way of this amendment. Full examination and favorable action are requested.

Please apply any charges not covered or any credits, to Deposit Account 50-0591 (Reference No. 09669/007001).

Respectfully submitted,

Date: 10/2/01

Jonathan P. Osha, Reg. No. 33,986
Rosenthal & Osha L.L.P.
700 Louisiana, Suite 4550
Houston, TX 77002

Telephone: (713) 228-8600
Facsimile: (713) 228-8778

19618_1.DOC

APPENDIX A – MARKED-UP VERSION OF THE AMENDED CLAIMS

(The material to be added is indicated by underlining, while the matter to be deleted is in brackets.)

1. An [Optical disk (10)] optical disk for storing data comprising a decryption module, [(20), that said module (20) including:] said module comprising:

   a memory [(22)] including at least one secret key [(K1)];

   a cryptoprocessor [(21)] to decrypt the data [(DATA)] of said disk [(10)] from said key [(K1),]; and

   a data exchange means [(IN_A, OUT_A, VCC_A, GRD_A)] for applying the data [(DATA)] of said disk [(10)] to the cryptoprocessor [(21)] and reading the decrypted data of the cryptoprocessor [(21)].

2. The [Optical] optical disk according to claim 1, characterised in that said decryption module [(20) is] comprises a chip with an integrated circuit.

3. The [Optical] optical disk according to claim 1, characterised in that said decryption module [(20)] is integrated in a central zone of said disk [(10)].

4. The [Optical] optical disk according to claim 1, characterised in that the data exchange means [(IN_A, OUT_A, VCC_A, GRD_A) are] is integrated in a central zone of the disk [(10)].

5. The [Optical] optical disk according to claim 1, characterised in that [it] said disk further comprises a balancing means [(E)] for balancing said disk.

6. The [Optical] optical disk according to claim 1, characterised in that the data exchange means [are] is fitted with contacts.

7. The [Optical] optical disk according to claim 1, characterised in that the data exchange means [are] is fitted with a means for transmitting an energy field.

8. A [Method] method for reading a data storage optical disk [(10)] comprising [a decryption module (20), said module (20) including:
a memory (22) including at least one key (K1);
a cryptoprocessor (21), and
data exchange means (IN_A, OUT_A, VCC_A, GRD_A),

said method including] the following stages:

an application stage in which [the] data [(DATA)] of said disk [(10)] are applied to [the] a cryptoprocessor [(21)] via [the] a data exchange means [(IN_A, OUT~A, VCC_A, CRD_A),];

a decryption stage in which the cryptoprocessor [(21)] decrypts the data [(DATA)] of said disk [(10)] from [said] a key [(K1),]; and

an extraction stage in which the decrypted data of the cryptoprocessor [(21)] are read via [the] a data exchange means [(IN A, OUT_A, VCC_A, GRD_A).];

wherein the optical disk comprises a decryption module, said module comprising a memory including at least one key, a cryptoprocessor, and a data exchange means.

9. The [Method] method according to claim 8, [characterised in that it comprises] further comprising an additional stage according to which:

prior to the decryption stage, the data [(DATA)] is modified into a format able to be understood by the cryptoprocessor by means of a cryptoprocessor interface [(37)] included in an optical disk reader.

10. The [Method] method according to claim 8, [characterised in that it comprises] further comprising an additional stage according to which:

prior to the decryption stage, the data [(DATA)] is modified into a format able to be understood by the cryptoprocessor by means of a cryptoprocerssor interface [(37)] included in a computer [(40)].

11. The [Method] method according to claim 8, characterised in that in the decryption stage the data [(DATA)] is systematically decrypted, whether said data is encrypted or not.

12. The [Method] method according to claim 8, [characterised in that it comprises] further comprising an additional stage according to which:

a set of unprocessed data [(B)] and a set of decrypted data [(D)] are loaded into a computer [(40)], both sets of data originating from a set of data read in the disk [(10)].

13. The [Method] method according to claim 12, characterised in that loading is made alternately.

14. The [Method] method according to claim 12, characterised in that a set of unprocessed data [(B) is composed of at last one] comprises a zone of unusable encrypted data [(Bb)], and a set of decrypted data [(D) is composed of at least one] comprises a zone of usable decrypted data [(Da)].

15. The [Method] method according to claim 12, characterised in that a set of unprocessed data [(B) is composed of at least one] comprises a zone of usable-non-encrypted data [(Ba)], and a set of decrypted data [(D) is composed of at least one] comprises a zone of unusable decrypted data [(Dd)].

16. The [Method] method according to claim 14 [or 15, characterised in that it comprises], further comprising an additional stage according to which:

an executable code portion in a useful data zone including application data is executed.

17. The [Method] method according to claim 16, [characterised in that it comprises] further comprising an additional stage according to which:

various data zones are interconnected, new data is loaded into the memory and a data zone is reconstituted with the aid of a set of links included in the executable code.

18. A [Disk] disk reader device [(30, 40)] placed to read an optical data storage disk [(10) as defined in claim 1], said device including an interface [(37, 38)] for exchanging data with [the] a decryption module [(20).], wherein the decryption module comprises a memory including at least one secret key, a cryptoprocessor to decrypt the data of said disk from said key, and a data exchange means for applying the data of said disk to the cryptoprocessor and reading the decrypted data of the cryptoprocessor.

19. A [Method] method for protecting an optical data storage disk [(10)] comprising [a decryption module (20) including:

a memory (22);

a cryptoprocessor (21), and

data exchange means (IN_A, OUT_A, VCC_A, GRD_A), the method including the following stages]:

an encryption stage in which [the] data is encrypted from at least one sole secret key [(Kl)] so as to obtain encrypted data;

a writing stage in which the encrypted data are written in said optical disk [(10),]; and

a loading stage in which the at least one key [or keys is/are] is loaded into [the] a memory [(22)] of [the] a decryption module [(20).]; wherein said optical data storage disk comprises a decryption module comprising a memory, a cryptoprocessor, and a data exchange means.

20. A [Method] method for protecting an optical disk [(10)] for storing data, [characterised in that the method comprises stages according to which]

comprising:

decrypting data [(DATA)] of said disk [(10) is decrypted] with the aid of a secret key [(K(1)] included in a memory [(22)] of a portable object [(20)] integrated in said disk and remaining inside said object during decryption,

exchanging the data [(DATA)] of said disk [(10) is exchanged] between said portable object [(20)] and said disk by means of data exchange means [(IN_A, OUT_A, VOW_A, GRD_A)] integrated in said disk.

21. The [Method] method according to claim 20, characterised in that said portable object [is] comprises a chip with an integrated circuit.

22. The [Method] method according to claim 20 [or 21], characterised in that the decryption stage is carried out using a cryptoprocessor integrated in said portable object [(20)].

23. The [Method] method according to claim 22, [characterised in that it comprises] further comprising an additional stage according to which:

prior to the decryption stage, the data [(DATA)] is modified into a format able to be understood by the cryptoprocessor via a cryptoprocessor [(37)] included in an optical disk reader.

24. The [Method] method according to claim 22, [characterised in that it comprises] further comprising an additional stage according to which:

prior to the decryption stage, the data [(DATA)] is modified into a format able to be understood by the cryptoprocessor by means of a cryptoprocessor interface [(37)] included in a computer [(40)].

25. The [Method] method according to [one of claims 20 to 24] claim 20, characterised in that the data [(DATA)] is decrypted systematically regardless of whether said data was originally encrypted or not.

26. The [Method] method according to [one of claims 20 to 25] claim 20,

[characterised in that it comprises] further comprising an additional stage according to which:

a set of unprocessed decrypted data [(D)] originating from a set of data read in the disk [(10)] is loaded into a computer [(40)].

27. The [Method] method according to claim 26, characterised in that loading is carried out alternately.

28. The [Method] method according to claim 26, characterised in that a set of unprocessed data [(B) is composed of at least one] comprises a zone of unusable encrypted data [(Bb)] and a set of decrypted data [(D) is composed of at least one] comprises a zone of usable decrypted data [(Da)].

29. The [Method] method according to claim 26, characterised in that a set of unprocessed data [(B) is composed of at least one] comprises a non-encrypted useful zone of data [(Ba)] , and a set of decrypted data [(D) is composed of at least one] comprises a zone of unusable decrypted data [(Dd)].

30. The [Method] method according to claim 28 [or 29], [characterised in that it comprises] further comprising an additional stage according to which:

one executable code portion included in the useful data zone is executed including application data.

31. The [Method] method according to claim 30, [characterised in that it comprises] further comprising an additional stage according to which:

[various] at least two data zones are interconnected, new data is loaded into the memory and a data zone is reconstructed with the aid of a set of links included in the executable code.

32. The [Method] method according to [one of claims 20 to 31] claim 20, [characterised in that it comprises] further comprising an additional stage according to which:

data is encrypted by means of a secret key [(K1)], wherein said encrypted data is written in said disk [(10)].

33. The [Method] method according to [one of claims 20 to 32] claim 20, [characterised in that it comprises] wherein said data [(DATA) forming] forms at least one application written in a high-level language.

34. The [Method] method according to claim 33, characterised in that the application is at least partially [or totally] encrypted.